Constabent Properties of Golay-Davis-Jedwab Sequences

M.G.Parker[1]

Code Theory Group,Institutt for Informatikk, University of Bergen,N-5020 Bergen, Norway

e-mail: matthew@ii.uib.no

Abstract — **We conjecture that length 2^t bipolar sequences with optimal or near-optimal Hadamard and Negahadamard Peak Factors are exactly the set of Golay Complementary sequences, as formed using the Davis-Jedwab construction. It appears Golay sequences are both Bent and Negabent for lengths 2^t where t is even and $t \neq 2 \bmod 3$. We also conjecture this sequence family has near-maximum distance from all constaaffine functions.**

I. Introduction

The sum of aperiodic autocorrelations of Golay sequence pairs is a δ pulse [2]. [1, 4] describe a construction for length 2^t Golay sequences (Golay-Davis-Jedwab construction (GDJ)) that probably covers all Golay sequences of length 2^t. We define Hadamard, Negahadamard and Constahadamard Transforms (HT, NHT and CHT), these being multidimensional Cyclic, Negacyclic and Constacyclic Discrete Fourier Transforms (DFT). Negabent and Constabent sequences are sequences whose NHTs and CHTs, respectively, have completely flat power profile. Extensive computation suggests that bipolar GDJ sequences always have flat or near-flat HTs, NHTs and CHTs. It is conjectured that these sequences are the unique intersection of the set of bipolar sequences with Bent or known near-Bent properties with those with NegaBent or known near-NegaBent properties. It is known that GDJ sequences are Bent for length 2^t, t even, [3], but the near-Bent property for length 2^t, t odd, and the Negabent and near-Negabent properties are new results. It is conjectured that bipolar GDJ sequences are both Bent and Negabent for a specified infinite set of lengths and therefore their associated boolean functions have maximum distance from affine and negaaffine functions. Further computations suggest they have near-maximum distance from all constaaffine functions in all cases. This may be desirable for cryptographic applications.

II. The Constahadamard Transform

The Walsh-Hadamard Transform (HT), $\mathbf{H_t}$, is constructed from the direct product of 2-point DFT matrices, $\mathbf{H_t} = \mathbf{H_1} \otimes \mathbf{H_1} \otimes \mathbf{H_1} \otimes \ldots = \otimes_{i=1}^{t} \mathbf{H_1}$ where $\mathbf{H_1} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$ and $\otimes$ is the direct product. The Negahadamard Transform (NHT), $\mathbf{NH_t}$, is the direct product of 2-point Discrete Negacyclic Fourier Transform matrices, $\mathbf{NH_t} = \mathbf{NH_1} \otimes \mathbf{NH_1} \otimes \mathbf{NH_1} \otimes \ldots = \otimes_{i=1}^{t} \mathbf{NH_1}$ where $\mathbf{NH_1} = \begin{pmatrix} 1 & i \\ 1 & -i \end{pmatrix}$, and $i^2 = -1$. The Constahadamard Transform (CHT), $\mathbf{C_{n,j}H_t}$, is the tth direct product of 2-point index j Discrete Constacyclic Fourier Transform (DCFT) matrices over nth complex roots where $2|n$, $\mathbf{C_{n,j}H_t} = \mathbf{C_{n,j}H_1} \otimes \mathbf{C_{n,j}H_1} \otimes \mathbf{C_{n,j}H_1} \otimes \ldots = \otimes_{i=1}^{t} \mathbf{C_{n,j}H_1}$ where $\mathbf{C_{n,j}H_1} = \begin{pmatrix} 1 & \alpha^j \\ 1 & \alpha^{j+\frac{n}{2}} \end{pmatrix}$, $\alpha = e^{\frac{2\pi ij}{n}}$, j is one of the $\frac{\phi(n)}{2}$ integers in Z_n mutually prime to n and less than $\frac{n}{2}$, and ϕ is Euler's Totient Function. e.g., $\mathbf{H_t} = \mathbf{C_{2,1}H_t}$, $\mathbf{NH_t} = \mathbf{C_{4,1}H_t}$, and, $\mathbf{C_{12,5}H_1} = \begin{pmatrix} 1 & \alpha^5 \\ 1 & \alpha^{11} \end{pmatrix}$, where $\alpha = e^{\frac{2\pi i}{12}}$.

Constahadamard Peak Factor: Let $\mathbf{A} = \mathbf{C_{n,j}H_t a} = (A_0, A_1, \ldots, A_{2^t-1})^T$ for some n, j. The Constahadamard Peak Factor of $\mathbf{a}$ is CHPF($\mathbf{a}$) $= 2^{-t}\max\{A_iA_i^*|0 \leq i < 2^t\}$. All CHT matrices obey Parseval's Theorem. $1.0 \leq$ CHPF($\mathbf{a}$) $\leq 2^t$ $\forall n, j$ if $\mathbf{a}$ is unimodular. A unimodular sequence is Bent if it has Hadamard Peak Factor (HPF) of 1.0, Negabent if it has Negahadamard Peak Factor (NHPF) of 1.0, and ConstaBent if it has CHPF of 1.0.

III. CHPF Properties of GDJ Sequences

GDJ Sequences are detailed in [1, 4]. They are certain second order cosets of Reed Muller $(1, t)$ which are length 2^t Golay Complementary Sequences. Bipolar GDJ sequences are bent for even t [3]. From computational results we state,

Conjecture 1: *The HPF of a bipolar GDJ sequence is* 1.0 *for even t and* 2.0 *for odd t.*

Conjecture 2: *The NHPF of a bipolar GDJ sequence is* 1.0 *for $t \neq 2$ mod 3 and* 2.0 *for $t = 2$ mod 3.*

Conjecture 3: *Bipolar GDJ sequences of length 2^t are both Bent and Negabent for even t, $t \neq 2$ mod 3.*

Conjecture 4: *Let $\mathbf{F}$ be the set of length 2^t bipolar sequences with HPF $= 1.0$ and 2.0 for t even and odd, respectively. Let $\mathbf{G}$ be the set of length 2^t bipolar sequences with NHPF $= 1.0$ and 2.0 for $t \neq 2$ mod 3 and $t = 2$ mod 3, respectively. The set of GDJ bipolar sequences is exactly $\mathbf{F} \cap \mathbf{G}$.*

Conjecture 5: *The CHPF of GDJ bipolar sequences is always ≤ 2.00, $\forall n, t, j$.*

Conjecture 3 follows from Conjectures 1 and 2. Conjecture 4 may not hold for t large. Conjecture 5 implies GDJ boolean functions have near-maximum distance from all constaaffine functions.

IV. Conclusion

Bipolar Golay-Davis-Jedwab (GDJ) sequences appear not only to possess low one-dimensional peak factors ≤ 2.0, but also possess low multi-dimensional peak factors ≤ 2.0. We conjecture these sequences are Bent or near-Bent and NegaBent or near-NegaBent. They appear to be Bent and Negabent for lengths 2^t, $t = 0$ or 4, mod 6.

References

[1] J.A.Davis,J.Jedwab, "Peak-to-mean Power Control in OFDM, Golay Complementary Sequences and Reed-Muller Codes," *HP Laboratories Tech. Rep.*, HP Laboratories Bristol, HPL-97-158, Dec '97

[2] M.J.E.Golay, "Complementary Series," *IRE Trans. Inform. Theory*, Vol IT-7, pp 82–87, Apr '61

[3] F.J.MacWilliams,N.J.A.Sloane, **The Theory of Error-Correcting Codes**, Amsterdam: North-Holland, '77

[4] K.G.Paterson, "Generalised Reed-Muller Codes and Power Control in OFDM Modulation," *HP Tech. Rep., HPL-98-57* March '98

[1] This work was funded by NFR Project Number 119390/431